HackeRoyale

Made With Love By h4ck0d3r for hAcKeRs...

Table Of Contents

All Nmap tool commands at your fingertips! 3
Best OS for hackers 9
How to be An0Nymous on Kali Linux by using Anonsurf module 17
How To Hack Any Wifi By WifiPhisher : Step-By-Step Tutorial 21
How to install Kali Linux on your Android 24
How to prepare for ethical hacking! 27

All Nmap tool commands at your fingertips!

by h4ck0d3r | Tuesday, December 06, 2016

Visit the article here http://www.hackeroyale.com/nmap-tool-commands/

> Hey mates, in this article I'm listing out here some of the most used nmap tool commands that can be used for foot-printing purposes. I've tried my best to sort out most of them. But if you find any missing, not mentioned here, that you know, you may text in the comment box below. This kind move of yours will surely add up-to knowledge of me & others.

Basic Scanning Techniques

Scan a single target —> nmap [target]

Scan multiple targets —> nmap [target1,target2,etc]

Scan a list of targets —-> nmap -iL [list.txt]

Scan a range of hosts —-> nmap [range of IP addresses]

Scan an entire subnet —-> nmap [IP address/cdir]

Scan random hosts —-> nmap -iR [number]

Excluding targets from a scan —> nmap [targets] –exclude [targets]

Excluding targets using a list —> nmap [targets] –excludefile [list.txt]

Perform an aggressive scan —> nmap -A [target]

Scan an IPv6 target —> nmap -6 [target]

Discovery Options

Perform a ping scan only —> nmap -sP [target]

Don’t ping —> nmap -PN [target]

TCP SYN Ping —> nmap -PS [target]

TCP ACK ping —-> nmap -PA [target]

UDP ping —-> nmap -PU [target]

SCTP Init Ping —> nmap -PY [target]

ICMP echo ping —-> nmap -PE [target]

ICMP Timestamp ping —> nmap -PP [target]

ICMP address mask ping —> nmap -PM [target]

IP protocol ping —-> nmap -PO [target]

ARP ping —> nmap -PR [target]

Traceroute —> nmap –traceroute [target]

Force reverse DNS resolution —> nmap -R [target]

Disable reverse DNS resolution —> nmap -n [target]

Alternative DNS lookup —> nmap –system-dns [target]

Manually specify DNS servers —> nmap –dns-servers [servers] [target]

Create a host list —-> nmap -sL [targets]

Advanced Scanning Options

TCP SYN Scan —> nmap -sS [target]

TCP connect scan —-> nmap -sT [target]

UDP scan —-> nmap -sU [target]

TCP Null scan —-> nmap -sN [target]

TCP Fin scan —> nmap -sF [target]

Xmas scan —-> nmap -sX [target]

TCP ACK scan —> nmap -sA [target]

Custom TCP scan —-> nmap –scanflags [flags] [target]

IP protocol scan —-> nmap -sO [target]

Send Raw Ethernet packets —-> nmap –send-eth [target]

Send IP packets —-> nmap –send-ip [target]

Port Scanning Options

Perform a fast scan —> nmap -F [target]

Scan specific ports —-> nmap -p [ports] [target]

Scan ports by name —-> nmap -p [port name] [target]

Scan ports by protocol —-> nmap -sU -sT -p U:[ports],T:[ports] [target]

Scan all ports —-> nmap -p “*” [target]

Scan top ports ——> nmap –top-ports [number] [target]

Perform a sequential port scan —-> nmap -r [target]

Version Detection

Operating system detection —-> nmap -O [target]

Submit TCP/IP Fingerprints —-> http://www.nmap.org/submit/

Attempt to guess an unknown —-> nmap -O –osscan-guess [target]

Service version detection —-> nmap -sV [target]

Troubleshooting version scans —-> nmap -sV –version-trace [target]

Perform a RPC scan —-> nmap -sR [target]

Timing Options

Timing Templates —-> nmap -T [0-5] [target]

Set the packet TTL —-> nmap –ttl Thursday, October 08, 2016 16:14 UTC+9 [target]

Minimum of parallel connections —-> nmap –min-parallelism [number] [target]

Maximum of parallel connection —-> nmap –max-parallelism [number] [target]

Minimum host group size ——> nmap –min-hostgroup [number] [targets]

Maximum host group size —-> nmap –max-hostgroup [number] [targets]

Maximum RTT timeout ——> nmap –initial-rtt-timeout Thursday, October 08, 2016 16:14 UTC+9 [target]

Initial RTT timeout —-> nmap –max-rtt-timeout [TTL] [target]

Maximum retries —-> nmap –max-retries [number] [target]

Host timeout —-> nmap –host-timeout Thursday, October 08, 2016 16:14 UTC+9 [target]

Minimum Scan delay —-> nmap –scan-delay Thursday, October 08, 2016 16:14 UTC+9 [target]

Maximum scan delay —-> nmap –max-scan-delay Thursday, October 08, 2016 16:14 UTC+9 [target]

Minimum packet rate —-> nmap –min-rate [number] [target]

Maximum packet rate —-> nmap –max-rate [number] [target]

Defeat reset rate limits —-> nmap –defeat-rst-ratelimit [target]

Firewall Evasion Techniques

Fragment packets —-> nmap -f [target]

Specify a specific MTU —-> nmap –mtu [MTU] [target]

Use a decoy —-> nmap -D RND: [number] [target]

Idle zombie scan —> nmap -sI [zombie] [target]

Manually specify a source port —-> nmap –source-port [port] [target]

Append random data —-> nmap –data-length [size] [target]

Randomize target scan order —-> nmap –randomize-hosts [target]

Spoof MAC Address —-> nmap –spoof-mac [MAC|0|vendor] [target]

Send bad checksums —-> nmap –badsum [target]

Output Options

Save output to a text file —-> nmap -oN [scan.txt] [target]

Save output to a xml file —> nmap -oX [scan.xml] [target]

Grepable output —-> nmap -oG [scan.txt] [target]

Output all supported file types —-> nmap -oA [path/filename] [target]

Periodically display statistics —-> nmap –stats-every Thursday, October 08, 2016 16:14 UTC+9 [target]

133t output —-> nmap -oS [scan.txt] [target]

Troubleshooting and debugging

Help —> nmap -h

Display Nmap version —-> nmap -V

Verbose output —-> nmap -v [target]

Debugging —-> nmap -d [target]

Display port state reason —-> nmap –reason [target]

Only display open ports —-> nmap –open [target]

Trace packets —> nmap –packet-trace [target]

Display host networking —> nmap –iflist

Specify a network interface —> nmap -e [interface] [target]

Nmap Scripting Engine

Execute individual scripts —> nmap –script [script.nse] [target]

Execute multiple scripts —-> nmap –script [expression] [target]

Script categories —-> all, auth, default, discovery, external, intrusive, malware, safe, vuln

Execute scripts by category —-> nmap –script [category] [target]

Execute multiple scripts categories —-> nmap –script [category1,category2, etc]

Troubleshoot scripts —-> nmap –script [script] –script-trace [target]

Update the script database —-> nmap –script-updatedb

Judging two outptus : Ndiff

Ndiff verbose mode —-> ndiff -v [scan1.xml] [scan2.xml]

Comparison using Ndiff —-> ndiff [scan1.xml] [scan2.xml]

XML output mode —-> ndiff –xml [scan1.xm] [scan2.xml]

You liked this article? Let me know in the comments below :)

Thank you!

****

Thank You for reading this article!

If you like our efforts, please contribute to us by giving your valuable feedback here

Keep visiting HackeRoyale for more cool stuffs...

Best OS for hackers

by h4ck0d3r | Saturday, December 03, 2016

Visit the article here http://www.hackeroyale.com/os-for-hackers/

> Hello everyone! Do you guess what are top best Operating Systems used by hackers?!
>
> Well, lets find out today...

Kali Linux

Kali Linux maintained and funded by Offensive Security Ltd. is first in our list. Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. Kali is the one of the best and favorite operating systems of hackers.

It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of BackTrack, their previous forensics Linux distribution based on Ubuntu. Kali Linux has a dedicated project set-aside for compatibility and porting to specific Android devices, called Kali Linux NetHunter. It is the first Open Source Android penetration testing platform for Nexus devices, created as a joint effort between the Kali community member “BinkyBear” and Offensive Security. It supports Wireless 802.11 frame injection, one-click MANA Evil Access Point setups, HID keyboard (Teensy like attacks), as well as Bad USB MITM attacks.

Visit official site here...

BlackArch Linux

BlackArch Linux -an Arch Linux-based penetration testing distribution for penetration testers and security researchers. The new version also has a total of 1400 penetration testing tools with the old ones updated and the new ones added, making it a must have download for hackers and security researchers.

Visit official site here...

Parrot Sec

Parrot Security OS (or ParrotSec) is a GNU/LINUX distribution based on Debian. It was built in order to perform penetration tests (computer security), Vulnerability Assessment and Mitigation, Computer Forensics and Anonymous Surfing. It has been developed by Frozenbox's Team. Like Kali Linux Parrot Security OS is also hackers favourite operating system.

Parrot is based on Debian's stable branch (jessie), with a custom hardened linux 4.1 kernel with a grsecurity patched branch available. It follows a development line of rolling release kind.The desktop environment is MATE, fork of Gnome 2, and the default display manager is LightDM.The project is certified to run over machines which have 265Mb of RAM at least and it is suitable to both 32bit (i386) and 64bit (amd64), with a special edition it works on old 32bit machines (486). Moreover, the project is available for armel and armhf architectures. It even offers an edition (both 32bit and 64bit) developed for servers only to carry out cloud pentesting.

Visit official site here...

BackBox

BackBox is an Ubuntu-based Linux distribution penetration test and security assessment oriented providing a network and informatic systems analysis toolkit. BackBox desktop environment includes a complete set of tools required for ethical hacking and security testing.

It includes some of the most used security and analysis Linux tools, aiming for a wide spread of goals, ranging from web application analysis to network analysis, from stress tests to sniffing, also including vulnerability assessment, computer forensic analysis and exploitation. Part of the power of this distribution comes from its Launchpad repository core, constantly updated to the latest stable version of the most known and used ethical hacking tools. The integration and development of new tools in the distribution follows the open source community, particularly the Debian Free Software Guidelines criteria.

Visit official site here...

Live Hacking OS

Live Hacking OS is a Linux distribution packed with tools and utilities for ethical hacking, penetration testing and countermeasure verification. It includes the graphical user interface GNOME inbuilt. There is a second variation available which has command line only, and it requires very less hardware requirements.

Download OS here...

Samurai Web Testing Framework

The Samurai Web Testing Framework is a live linux environment that has been pre-configured to function as a web pen-testing environment. The CD contains the best of the open source and free tools that focus on testing and attacking websites. In developing this environment, we have based our tool selection on the tools we use in our security practice. We have included the tools used in all four steps of a web pen-test.

Visit official site here...

DEFT

DEFT stands for Digital Evidence and Forensic Toolkit and it’s an open source distribution of Linux built around the DART (Digital Advanced Response Toolkit) software and based on the Ubuntu operating system. It has been designed from the ground up to offer some of the best open source computer forensics and incident response tools that can be used by individuals, IT auditors, investigators, military, and police.

Visit official site here...

Bugtraq

Bugtraq is an electronic mailing list dedicated to issues about computer security. On-topic issues are new discussions about vulnerabilities, vendor security-related announcements, methods of exploitation, and how to fix them. It is a high-volume mailing list, and almost all new vulnerabilities are discussed there.Bugtraq team is experienced freaks and developers, It is available in Debian, Ubuntu and OpenSuSe in 32 and 64 bit architectures.

Visit official site here...

NodeZero

NodeZero is an open source Linux kernel-based operating system derived from the world's most popular distribution of Linux, Ubuntu, and designed to be used for penetration testing operations. The distro is available for download as a dual-arch Live DVD ISO image, which will run well on computers that support both 32-bit (x86) and 64-bit (x86_64) instruction set architectures. Besides the fact that it allows you to start the live system, the boot menu contains various advanced options, such as the ability to perform a system memory diagnostic test, boot from a local drive, start the installer directly, as well as to boot in safe graphics mode, text mode or debug mode.

NodeZero's default graphical desktop environment is powered by GNOME, which uses the GNOME Classic interface. It features a two-panel layout, and uses Ubuntu's default software repositories. Keep in mind though, that you must first log into the live session with the username nodezero and without a password.With NodeZero you will have instant access to over 300 penetration testing tools, as well as a set of basic services that are needed in penetration testing operations. Default applications include the Mozilla Firefox web browser, F-Spot photo manager, Rhythmbox music player, PiTiVi video editor, Transmission torrent downloader, Empathy multi-protocol instant messenger, and OpenOffice.org office suite.

Dwonload OS here...

Pentoo

Pentoo is a Live CD and Live USB designed for penetration testing and security assessment. Based on Gentoo Linux, Pentoo is provided both as 32 and 64 bit installable livecd. Pentoo is also available as an overlay for an existing Gentoo installation. It features packet injection patched wifi drivers, GPGPU cracking software, and lots of tools for penetration testing and security assessment. The Pentoo kernel

includes grsecurity and PAX hardening and extra patches – with binaries compiled from a hardened toolchain with the latest nightly versions of some tools available.

Visit official site here...

Cyborg Hawk Linux

CYBORG HAWK LINUX is a Ubuntu (Linux) based Penetration Testing Distro created by the team of Ztrela Knowledge Solutions Pvt. Ltd. Developed and designed for ethical hackers and cyber security experts who are also known as Penetration testers . Cyborg Hawk Penetration Testing Distro can be used for network security and assessment and also for digital forensics. It has various tools also fit for the Mobile Security and Wireless testing. It has 700 + tools while other penetration distro have 300+ and also dedicated tools for and menu for mobile security and malware analysis . Also it is easy to compare it with others as to make a better OS than others ,we have to outperform them.

Visit official site here...

Download OS here...

Network Security Toolkit

The Network Security Toolkit (NST) is a Linux-based Live CD that provides a set of open source computer security and networking tools to perform routine security and networking diagnostic and monitoring tasks. The distribution can be used as a network security analysis, validation and monitoring tool on servers hosting virtual machines. The majority of tools published in the article “Top 125 security tools” by Insecure.org are available in the toolkit. NST has package management capabilities similar to Fedora and maintains its own repository of additional packages.

Features : Many tasks that can be performed within NST are available through a web interface called NST WUI. Among the tools that can be used through this interface are nmap with the vizualization tool ZenMap, ntop, a Network Interface Bandwidth Monitor, a Network Segment ARP Scanner, a session manager for VNC, a minicom-based terminal server, serial port monitoring, and WPA PSK management.Other features include visualization of ntopng, ntop, wireshark, traceroute, netflow and kismet data by geolocating the host addresses, IPv4 Address conversation, traceroute data and wireless access points and displaying them via Google Earth or a Mercator World Map bit image, a browser-based

packet capture and protocol analysis system capable of monitoring up to four network interfaces using Wireshark, as well as a Snort-based intrusion detection system with a “collector” backend that stores incidents in a MySQL database. For web developers, there is also a JavaScript console with a built-in object library with functions that aid the development of dynamic web pages.

Visit official site here...

Knoppix STD

STD is a Linux-based Security Tool. Actually, it is a collection of hundreds if not thousands of open source security tools. It’s a Live Linux Distro, which means it runs from a bootable CD in memory without changing the native operating system of the host computer. Its sole purpose in life is to put as many security tools at your disposal with as slick an interface as it can.STD is meant to be used by both novice and professional security personnel but is not ideal for the Linux uninitiated. STD assumes you know the basics of Linux as most of your work will be done from the command line. If you are completely new to Linux, it’s best you start with another live Distro like Knoppix to practice the basics.STD tools are divided into the following categories
authentication, encryption, forensics, firewall, honeypot, ids, network utilities, password tools, servers, packet sniffers, tcp tools, tunnels, vulnerability assessment, wireless tools.

Visit official site here...

Weakerthan

Weakerthan is a penetration testing distribution which is built from Debian Squeeze.For the desktop environment it uses Fluxbox.This operating system is ideal for WiFi hacking as it contains plenty of Wireless tools. It has a very well maintained website and a devoted community. Built from Debian Squeeze (Fluxbox within a desktop environment) this operating system is particularly suited for WiFi hacking as it contains plenty of Wireless cracking and hacking tools.Tools includes: Wifi attacks, SQL Hacking, Cisco Exploitation, Password Cracking, Web Hacking, Bluetooth, VoIP Hacking, Social Engineering, Information Gathering, Fuzzing Android Hacking, Networking and creating Shells.

Visit official site here...

Matriux Linux

Matriux Linux – a Debian-based security distribution designed for penetration testing and forensic investigations. Although suited best for hackers, it can also be used by any Linux user as a desktop system for day-to-day computing. Matriux has more than 300 open source tools for penetration testing and hacking. Since its the new one, many security researchers claims that it is a better alternative to Kali Linux.

Visit official site here...

GnackTrack

GnackTrack is an open and free project to merge penetration testing tools and the linux Gnome desktop. GnackTrack is a Live and comes with multiple tools that are really helpful to do a effective penetration testing, it has Metasploit, armitage, wa3f and others wonderful tools.

Download OS here...

BlackBuntu

BlackBuntu is distribution for penetration testing which was specially designed for security training students and practitioners of information security. BlackBuntu is penetration testing distribution with GNOME Desktop Environment. It’s currently being built using the Ubuntu 10.10 and work on reference BackTrack.

Caine

Caine is an Ubuntu-based security-focused distro that is available as a live disk. It stands for Computer Aided Investigation Environment and can also be run from the hard disk after installation. This Linux distro comes with a wide range of tools to help you in system forensics.

Caine comes with a large number of database, memory, forensics, and network analysis applications. This distro for ethical hacking also features common applications like web browsers, email clients, document editors etc. for usual computing purposes.

Visit official site here...

I hope friends you really liked reading this tutorial. Please do like, comment & share with others too! And yeah, don't forget to check my other posts too!

//assets.pinterest.com/js/pinit.js

****

Thank You for reading this article!

If you like our efforts, please contribute to us by giving your valuable feedback here

Keep visiting HackeRoyale for more cool stuffs...

How to be An0Nymous on Kali Linux by using Anonsurf module

by h4ck0d3r | Saturday, December 03, 2016

Visit the article here http://www.hackeroyale.com/anonsurf-kali-linux/

> Hey guys, today I'm gonna show you all a very quick, easy & effective method to remain anonymous on your Kali Linux system so that no one can trace you from your activities.

Also Read: Kali Linux on your Android

So, basically, we're gonna install Anonsurf module, which will anonymize the entire system under TOR using IPTables.

STEP 1: Download Anonsurf.

Fire up your kali & enter following command in terminal.

```
git clone https://github.com/Und3rf10w/kali-anonsurf.git
```

---

root@kali:~# git clone https://github.com/Und3rf10w/kali-anonsurf.git

Cloning into 'kali-anonsurf'...

remote: Counting objects: 275, done.

remote: Total 275 (delta 0), reused 0 (delta 0), pack-reused 275

Receiving objects: 100% (275/275), 163.44 KiB | 75.00 KiB/s, done.

Resolving deltas: 100% (79/79), done.

Checking connectivity... done.

root@kali:~#

After the download is complete, goto to the directory where you downloaded. You can do this by using `cd` command to move back & forth through various directories.

---

root@kali:~#

root@kali:~# cd kali-anonsurf/

root@kali:~/kali-anonsurf#

root@kali:~/kali-anonsurf# ls

installer.sh kali-anonsurf-deb-src LICENSE README.md

root@kali:~/kali-anonsurf#

STEP 2: Install Anonsurf.

In the kali-anonsurf folder, you'll find an installer script. Kudos, that's what we want to get anonsurf working on your system.

So now, simply execute the script by entering the following command:

```
./installer.sh
```

Now it will automatically install the module onto your system & it will also update the */etc/tor/torrc* file to add the following code.

VirtualAddrNetwork 10.192.0.0/10

AutomapHostsOnResolve 1

TransPort 9040

SocksPort 9050

DNSPort 53

RunAsDaemon 1

It will also update your */etc/resolv.conf* file to update the following code.

---

root@kali:~# cat /etc/resolv.conf

nameserver 127.0.0.1

nameserver 209.222.18.222

nameserver 209.222.18.218

STEP 3: Run Anonsurf.

So, with this anonsurf installed, now you are all set to start it.

Enter the following command whenever you want to begin the process. It will automatically start TOR

for you.

```
anonsurf start
```

root@kali:~# anonsurf start

* killing dangerous applications

* cleaning some dangerous cache elements

[i] Stopping IPv6 services:

[i] Starting anonymous mode:

* Tor is not running! starting it for you

* Saved iptables rules

* Modified resolv.conf to use Tor and Private Internet Access DNS

* All traffic was redirected throught Tor

[i] You are under AnonSurf tunnel

root@kali:~#

Now, you can also check your IP by the following command:

```
anonsurf myip
```

root@kali:~# anonsurf myip

My ip is:

1xx.1xx.2xx.1xx

To stop anonsurf, simply type in the following:

```
anonsurf stop
```

root@kali:~# anonsurf stop

* killing dangerous applications

* cleaning some dangerous cache elements

[i] Stopping anonymous mode:

* Deleted all iptables rules

* Iptables rules restored

[i] Reenabling IPv6 services:

* Anonymous mode stopped

Instead of stopping and starting again, you can simply restart it to avoid the painstaking. Just hit the following command:

```
anonsurf restart
```

So, each time you restart anonsurf, it will randomly assign you a different IP address! Isn't that amazing & cool guys?!

Also Read:

How to stay anonymous while hacking (Part 1)

How to stay anonymous while hacking (Part 2)

WARNING: Don't ever run anonsurf by `service anonsurf start` command. Run it as `anonsurf start`

Just to satisfy yourself, you may check your IP & DNS by visiting the following site:

https://www.whatismyip.com/

http://dnsleak.com

That's it guys, I hope you enjoy reading this tutorial. Please comment below whether you liked it or not. Your feedbacks value a lot for us. Meet you soon guys! Take care & happy winter. :)

****

Thank You for reading this article!

If you like our efforts, please contribute to us by giving your valuable feedback here

Keep visiting HackeRoyale for more cool stuffs...

How To Hack Any Wifi By WifiPhisher : Step-By-Step Tutorial

by sam | Sunday, January 29, 2017

Visit the article here http://www.hackeroyale.com/wifi-hacking/

Hello guys today I am going to show you WiFi hacking using Phishing method.

You may also like to read hacking WiFi using the Wps Push Button here.

So follow me:

First step to WiFi Hacking

Installing WifiPhisher!

To begin, fire up Kali and open a terminal. Then download Wifiphisher from GitHub and unpack the code.

```
kali> tar -xvzf /root/wifiphisher-1.1.tar.gz
```

As you can see below, I have unpacked the Wifiphisher source code.

STEP 2

Navigate To The Directory

Next, navigate to the directory that Wifiphisher created when it was unpacked. In my case, it is ***/wifiphisher-1.1***.

```
kali> cd wifiphisher-.1.1
```

When listing the contents of that directory, you will see that the **wifiphisher.py** script is there.

```
kali>ls -l
```

STEP 3

Run The Script

You can run the Wifiphisher script by typing:

```
kali> python wifiphisher.py
```

Note that I preceded the script with the name of the interpreter, **python**.

The first time you run the script, it will likely tell you that "**hostapd**" is not found and will prompt you to install it. Install by typing "**y**" for yes. It will then proceed to install hostapd.

When it has completed, once again, execute the Wifiphisher script.

```
kali> python wifiphisher.py
```

This time, it will start the web server on **port 8080** and **443**, then go about and discover the available Wi-Fi networks.

When it has completed, it will list all the Wi-Fi networks it has discovered. Notice at the bottom of my example that it has discovered the network "wonder how to". That is the network we will be attacking.

STEP 4

Send Your Attack & Get The Password

Go ahead and hit **Ctrl + C** on your keyboard and you will be prompted for the number of the **AP (Access Point)** that you would like to attack. In my case, it is 12.

When you hit **Enter**, Wifiphisher will display a screen like the one below that indicates the interface being used and the SSID of the AP being attacked and cloned.

The target user has been de-authenticated from their AP. When they re-authenticate, they will directed to the cloned evil twin access point.

When they do, the proxy on the web server will catch their request and serve up an authentic-looking message that a firmware upgrade has taken place on their router and they must re-authenticate.

Notice that I have not entered my password.

When the user enters their password, it will be passed to you through the Wifi phisher open terminal.

Read my tutorial here on building strong passwords to add up-to your defense strategies against malicious attacks!

The user will be passed through to the web through your system and out to the Internet, never suspecting anything awry has happened.

****

Thank You for reading this article!

If you like our efforts, please contribute to us by giving your valuable feedback here

Keep visiting HackeRoyale for more cool stuffs...

How to install Kali Linux on your Android

by h4ck0d3r | Saturday, December 03, 2016

Visit the article here http://www.hackeroyale.com/kali-linux-on-android/

> Hello guys, today I'm going to share you the process of installing Kali Linux on your Android Smartphone.
>
> Before moving on, lets get handy with all that you need to get Kali Linux working on your Android.

1. **A device running Android 2.1 and above, rooted.**
2. **Rooted Android device.**
3. **At least 5 GB free space on internal or external storage.**
4. **Completely charged Android device.**
5. **Busybox App.** Download here.
6. **Linux Deploy.** Download here.
7. **Android VNC Viewer.** Download here.
8. **A fast internet connection.**
9. **Last but not least, patience.**

Also Read: How to root any Android in 2 minutes

Step 1:

First we need to install UNIX Scripts into our device using Busybox App. Download and install the app.

Step 2:

Setting up Linux Deploy:

- **First of all download and install Linux Deploy App on your device from Google Play Store.**
- **Now after downloading and installing it launch the app in your device and there tap on the download button.**
- **Now there tap on Distribution option and change it to Kali Linux.**
- **Now scroll up and click on the Install button at the top of there.**
- **Now wait for the download to finish, it requires time depending upon your internet speed.**

Step 4:

- **Now download and install VNC Viewer App in your Android from Play Store.**
- **Now launch the VNC Viewer App and fill up the settings.**
- **Now click on Connect button there.**

Also Read: Anonsurf module installation for Kali Linux

Now you're done and you will be able to run Kali Linux on your Android device!

Thank you for reading this article...

****

Thank You for reading this article!

If you like our efforts, please contribute to us by giving your valuable feedback here

Keep visiting HackeRoyale for more cool stuffs...

How to prepare for ethical hacking!

by h4ck0d3r | Tuesday, December 20, 2016

Visit the article here http://www.hackeroyale.com/ethical-hacking-preparation/

Hello, what I've seen here on HackeRoyale is that many newcomers want to hack the web and do some black-hat things, that's fine for me but I don't recommend you to. Ethical hacking requires patience & practice with it. Since the cost of a dumped database is pretty darn expensive and the owner will do anything to get that money from you with a law suite.

You might also forget that there are hackers out there that might be targeting YOU right now! So you might want to secure your system before you even think about taking that black hat on and go offensive on the internet. Tackling with these cruel elements is a bet! That's where Ethical Hacking comes into picture!

So I'll try to point the beginners in the right direction here, to make your system more secure.

More articles for beginners here:

Notice I wrote "more secure", because when you think "I'm safe and sound" you're wrong, there is always a way in, and you should be aware of that.

Check my previous articles on how to stay anonymous while hacking!

How to stay anonymous while hacking (Part 1)

How to stay anonymous while hacking (Part 2)

Tightening your belts for Ethical Hacking!

Use a trustworthy VPN service provider!

It's hard to find a good VPN service that doesn't log your IP address today, so you have to find a service that you trust!

You can find a really great VPN comparison chart on the following link
https://thatoneprivacysite.net/vpn-comparison-chart/

A VPN stands for Virtual private network and acts like a tunnel for your connection. In short, your ISP will only see traffic to the VPN servers and from there the data is invisible for the ISP. This goes for website owners as well, they will only see the VPN service IP in the logs when you visit their site.

Use a firewall to filter out bad incoming/outgoing traffic

A firewall is pretty much a must have to secure your system from unwanted incoming traffic such as a targeted attack or a RAT (Remote administration tool) for example. I won't explain what a firewall is doing in depth since I bet you have the basic understanding of what a firewall does to secure your network/system.
What I will do is to give you an advice to download a free and great free firewall here if you don't use one today or want to use a firewall that is doing the job with less system requirements!
Glasswire is the name, and you can read more about it here and download it on the following link.

https://www.glasswire.com/

Stay safe from malware/virus

Use anti malwarebytes and scan the system frequently (at least once a week) to stay safe from most malwares that might have gotten in to your system. An active antivirus software is good, but not a must if you know what you're doing. I've been using my system a long time without any AV now and that is because I stay aware of what I click on and use a virtual machine for weird stuff that I want to run/install.

Also Read: How Does Anti-virus Works?

You should use add-ons to Firefox and chrome to make the web more secure while surfing as well.

HTTPS everywhere

Privacy Badger

WebRTC Leak prevent

uBlock origin

So what is a virtual machine?

It's in short a computer running virtually inside of your system. If you get a virus on that machine and totally lose control of it, you can just shut it down and reinstall it without your main system getting infected.
You can download VMware player or virtual box and install any system you like to it.

Link to VMware workstation player
https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0

Link to VirtualBox

https://www.virtualbox.org/wiki/Downloads

Let’s say you want to run Kali Linux 2 in VMware player! You just download the kali image file from

the following link. This image is ready to go directly in VMware player without any installation. Really fast and easy!
Just do as I did in the picture and find to the kali Linux vmdk file to run.

Download the Kali Linux 2.0 image here:

https://www.kali.org/downloads/

There are a lot of ISO files out there for almost any OS, so you can set up an windows machine for pen testing.

You can also install Kali Linux on your Android device too. Read here:

How to install Kali Linux on your Android

This is some very basic security measures that you should be using as a beginner for ethical hacking. I hope you learned something and I will try to answer any questions that you might have.

Of course there is more than just this, like system encryption and encrypted containers for securing your personal data as well. But I think that it is a whole new tutorial since it's too much to go through.

Have a great day!

****

Thank You for reading this article!

If you like our efforts, please contribute to us by giving your valuable feedback here

Keep visiting HackeRoyale for more cool stuffs...

HackeRoyale

Made With Love By h4ck0d3r for hAcKeRs...